IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claims 4 and 12-20; AMEND claims 1-3 and 5-11 and ADD new claims 21-23 in accordance with the following:

1. (currently amended) A method for ~~forming~~ producing a ~~secret~~ regenerated ~~communication~~ private key by a computer for a predetermined asymmetric cryptographic key pair which ~~comprises~~ includes an original private key and a corresponding public key, ~~by a computer,~~ the regenerated private key being identical to the original private key, the original private key and the public key having been generated by receiving a predetermined initial value entered by a user; processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers; checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value; repeating the step of checking until the first and second prime numbers are obtained; storing an index to obtain a stored index, the stored index being a number indicating how often, in the step of checking, the base value has been increased until the first prime number or the second prime number are obtained; calculating the original private key using the first and second prime numbers; and calculating the public key using the original private key and the first and second prime numbers, the method comprising: ~~the steps of: utilizing a prescribable initial value given a determination of said key pair; providing said initial value to a user; entering, by said~~

receiving a user~~, said~~ input of the predetermined initial value ~~into said~~ by the computer;

processing the predetermined initial value to obtain a base value for obtaining the first and second prime numbers;

increasing the base value by a value determined by the index previously stored and the predetermined increment to obtain the first and second prime numbers; and ~~forming said~~

calculating the regenerated private ~~secret communication~~ key ~~upon utilization of said initial value, said secret communication key and said public key forming an asymmetric cryptographic communication key pair~~ using the first and second prime numbers.

2. (currently amended) The method according to claim 1, ~~further comprising the steps of: supplying said~~

wherein, when obtaining the original private key, the predetermined initial value is supplied to a hash function to obtain the base value; and ~~determining, using a~~

wherein, when obtaining the regenerated private key, the same hash function ~~value formed by said hash function, said key pair and said communication key pair~~ is used.

3. (currently amended) The method according to claim 1, ~~further comprising the step of: including additional data characterizing said user when said key pair and said communication key pair are formed~~

wherein, when obtaining the original private key, the predetermined initial value is supplied to a hash function to obtain the base value, and

wherein, when obtaining the regenerated private key, the same hash function is used in the step of processing the, and

the respective values formed by the hash function are used in the determination of both an original key pair and a regenerated key pair.

4. (cancelled)

5. (currently amended) The method according to claim 41, wherein, when generating the original private key and the public key, ~~said determination of primacy for any given number is carried out according to the method of~~of the method of Miller-Rabin is used when checking whether the base value is a prime number.

6. (currently amended) The method according to claim 1,

wherein the asymmetric cryptographic key ~~keys are~~pair is formed according to the RSA method.

7. (currently amended) The method according to claim 2, wherein ~~said~~the hash function is ~~selected from the group consisting~~one of the following ~~of the~~ methods:

- MD-5 method,

- the MD-2 method, and

~~-the Data Encryption Standard~~method according to the data encryption standard (DES) ~~method~~ as a one-way function.

8. (currently amended) The method according to claim 1, further comprising the following ~~step of~~:

~~enciphering~~using the regenerated private key for encryption electronic data ~~with said secret communication key~~.

9. (currently amended) The method according to claim 1, further comprising ~~the step of~~:

~~forming a digital signature via electronic data using said secret communication key~~ using the regenerated private key for forming a digital signature.

10. (currently amended) The method according to claim 1, further comprising the following step ~~of~~:

~~authenticating data using said~~using the regenerated private key for an authentication ~~secret communication key~~.

11. (currently amended) A~~n arrangement for forming~~system to form a ~~secret communication key~~regenerated private key for a predetermined asymmetric cryptographic key pair, which ~~comprises a private key and a corresponding public key, comprising:~~

~~an input device configured for entering an initial value by a user; and~~

~~a processor connected to said input device, said processor configured to:~~

~~determine, using said prescribable initial value, said asymmetric cryptographic key pair;~~

~~accept entry of said initial value made available to said user; and~~

~~form said secret communication key using said initial value, where said secret communication key and said public key form a communication key pair~~includes an original private key and a corresponding public key, the regenerated private key being identical to the original private key, the original private key and the public key having been generated by receiving a predetermined initial value entered by a user; processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers; checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value; repeating the step of checking until the first and second prime numbers are obtained; storing an index to obtain a stored index, the stored index being a number indicating how often, in the step of checking, the base value

has been increased until the first prime number or the second prime number are obtained; calculating the original private key using the first and second prime numbers; and calculating the public key using the original private key and the first and second prime numbers, the system comprising:

an input device to receive a user input of the predetermined initial value;

a processor to process the predetermined initial value to obtain the base value for obtaining the first and second prime numbers, to increase the base value by a value determined by the stored index and the predetermined increment to obtain the first prime number or the second prime number; and to produce the regenerated private key using the first prime number and the second prime number.

Claims 12-20 (Cancelled)

21. (New) A method for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:

receiving a predetermined initial value entered by a user;

processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers;

checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value;

repeating the step of checking, until the first and second prime numbers are obtained,

storing an index indicating how often, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained;

calculating the private key using the first prime number and the second prime number;

calculating the public key using the private key, the first prime number and the second prime number; and

erasing the private key.

22. (New) A method in accordance with claim 21, wherein

the private key is used in a cryptographic operation, and

erasing is performed after using the private key in the cryptographic operation.

23. (New) An apparatus for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:

means for receiving a predetermined initial value entered by a user;

means for processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers;

means for checking, whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value;

means for repeating the step of checking, until the first and second prime numbers are obtained,

means for storing an index indicating how often, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained;

means for calculating the private key using the first prime number and the second prime number;

means for calculating the public key using the private key, the first prime number and the second prime number; and

means for erasing the private key.